UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/500,108	02/08/2000	Kevin L. Fox	GCSD-1054 (51045)	2137

7590 05/04/2004

Richard K Warther
Allen Dyer Doppelt Milbrath & Gilchrist PA
255 S Orange Avenue - Suite 1401
P O Box 3791
Orlando, FL 32802-3791

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/04/2004

17

Please find below and/or attached an Office communication concerning this application or proceeding.

7

Office Action Summary	Application No.	Applicant(s)	
	09/500,108	FOX ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *09 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6.11.12*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the arguments filed on February 9, 2004, Paper No. 13. Original application contained claims 1-36. Applicant filed an affidavit under 37 CFR 1.131. Presently pending claims are 1-36.

Response to Amendment

2. The affidavit filed on February 9, 2004 under 37 CFR 1.131 has been considered but is ineffective to overcome the Gleichauf et al. (U.S. Patent 6,415,321) reference.

The evidence submitted is insufficient to establish a conception of the invention prior to the effective date of the Gleichauf (U.S. Patent 6,415,321) reference. While conception is the mental part of the inventive act, it must be capable of proof, such as by demonstrative evidence or by a complete disclosure to another. Conception is more than a vague idea of how to solve a problem. The requisite means themselves and their interaction must also be comprehended. See *Mergenthaler v. Scudder*, 1897 C.D. 724, 81 O.G. 1417 (D.C. Cir. 1897). There is not sufficient evidence on the exhibits supplied by the applicants to demonstrate that the work was completed before the filing date of the Gleichauf reference, and therefore the reference will not be removed as a reference unless the applicant provides more discrete evidence demonstrating that the invention was conceived before the effective filing date of the Gleichauf (U.S. Patent 6,415,321) reference. For example, exhibits 1-6 should have a date of publication

associated with them so that it can be ascertained that the documents were conceived before the filing date of the Gleichauf reference (U.S. Patent 6,415,321).

Response to Arguments

3. Applicant's arguments filed February 9, 2004 have been fully considered but they are not persuasive for the following reasons:

The applicants in regards to claims 1 – 36, argue that the cited prior art [Gleichauf U.S. Patent 6,415,321] does not teach "the use of disparate network vulnerability analysis programs." This argument is not found persuasive. Gleichauf discloses a vulnerability/risk analysis procedure (Figure 1 step 5), which assesses different vulnerabilities gathered by passive, active, or query processing. The applicant states, "current generation risk analysis tools are usually single vendor solutions that address a particular aspect or aspects of risk" (Page 3 lines 5 – 10). Gleichauf discloses a system that each device has an ability to perform disparate vulnerability assessment of the network (column 4 lines 32 – 47). Furthermore, Gleichauf discloses a system that provides potential vulnerabilities/risks associated with programs, devices, and operating systems, which are disparate, network vulnerability assessments (column 5 lines 15 – 31).

The applicant's argument pertaining to Mayo et al. (U.S. Patent 5,751,965) is also not found persuasive. The applicant argues that Mayo does not suggest "assessing a

security posture of a network by creating a system object model database, exporting the database to disparate network vulnerability/risk analysis programs, analyzing the network, and correlating data results to determine the security posture of the network." However, the examiner never claimed that Mayo teaches the aforementioned aspects of applicant's invention, but that Mayo teaches a graphical user interface, which by the applicant's admission, it does.

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the subject matter "the use of disparate network vulnerability analysis programs" broadly recited in the independent claims 1, 7, 13, 19, 25, and 31. The dependent claims 2-6, 8-12, 14-18, 20-24, 26-30, and 32-36 are rejected at least by virtue of their dependency on the independent claims and by other reason set forth in the previous office action (Paper No. 9). Accordingly, the rejections for claims 1-36 are maintained as follows.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,2,4,6,7,8,10,12,13,14,16,18,19,20,22,24,25,29,31 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Gleichauf et al. (U.S. Patent No. 6,415,321).

Regarding claim 1, Gleichauf discloses:

A method for assessing the security posture of a network comprising the steps of:

creating a system object model database representing a network, wherein the system object model database supports the information data requirements of disparate network vulnerability analysis programs (column 5 lines 36-45);

exporting the system object model database of the network to the disparate network vulnerability/risk analysis programs (column 5 lines 36-60, column 7 lines 1-9);

analyzing the network with each network vulnerability analysis program to produce data results from each program (column 2 lines 64-67, column 3 lines 1-9); and

correlating the data results of the network vulnerability analysis programs to determine the security posture of the network (column 5 lines 55-58, column 6 lines 44-47).

Regarding claim 7, Gleichauf discloses:

A method for assessing the security posture of a network comprising the steps of:

creating a system object model database representing a network, wherein the system object model database supports the information data requirements of network vulnerability/risk analysis programs (column 5 lines 36-45);

importing the system object model database of the network to the network vulnerability analysis programs through filters associated with each respective network vulnerability analysis programs to export only the data required by a respective network vulnerability analysis program (column 5 lines 36-60, column 7 lines 1-9);

analyzing the network with each network vulnerability analysis program to produce data results from each program (column 2 lines 64-67, column 3 lines 1-9); and

correlating the data results of the network vulnerability analysis programs to determine the security posture of the network (column 5 lines 55-58, column 6 lines 44-47).

Regarding claim 13, Gleichauf discloses:

A computer program that resides on a medium that can be read by a program, wherein the computer program comprises instructions to cause a computer to:

create a system object model database representing a network, wherein the system object model database supports the information data requirements of disparate network vulnerability analysis programs that analyze discrete network portions (column 5 lines 36-45);

export the system object model database of the network to the network vulnerability analysis programs (column 5 lines 36-60, column 7 lines 1-9);

analyze the network with each network vulnerability/risk analysis program to produce data results from each program (column 2 lines 64-67, column 3 lines 1-9); and

correlate the data results of the network vulnerability analysis programs to determine the security posture of the network (column 5 lines 55-58, column 6 lines 44-47).

Regarding claim 19, Gleichauf discloses:

A computer program that resides on a medium that can be read by a program, wherein the computer program comprises instructions to cause a computer to:

create a system object model database representing a network, wherein the system object model database supports the information data requirements of disparate network vulnerability analysis programs that analyze discrete network portions (column 5 lines 36-45);

import the system object model database of the network to the network vulnerability analysis programs through filters associated with each respective network vulnerability analysis program so as to export only the data required by the respective network vulnerability analysis program (column 5 lines 36-60, column 7 lines 1-9);

analyze the network with each network vulnerability analysis program to produce data results from each program (column 2 lines 64-67, column 3 lines 1-9); and correlate the data results of the network vulnerability analysis programs to determine the security posture of the network (column 5 lines 55-58, column 6 lines 44-47).

Regarding claim 25, Gleichauf discloses:

A data processing system for assessing the security vulnerability of a network comprising:

a plurality of disparate network vulnerability/risk analysis programs used for analyzing a network (column 3 lines 1-10, column 5 lines 36-45);

a system object model database that represents the network to be analyzed, wherein the system object model database supports the information data requirements of the network vulnerability/risk analysis programs (column 5 lines 36-45);

an applications programming interface for exporting the system object model database of the network to the network vulnerability/risk analysis programs (column 2 lines 58-63, column 5 lines 36-41, column 6 lines 48-50); and

a processor for correlating the data results obtained from each network vulnerability analysis program after analyzing the network to determine the security posture of the network (column 5 lines 55-58, column 6 lines 44-47).

Regarding claim 31, Gleichauf discloses:

A data processing system for assessing the security vulnerability of a network comprising:

a plurality of disparate network vulnerability/risk analysis programs used for analyzing a network;

a system object model database that represents the network to be analyzed, wherein the system object model database supports the information data requirements of each network vulnerability analysis program (column 5 lines 36-45);

an applications programming interface for exporting the system object model database of the network to the disparate network vulnerability analysis programs (column 2 lines 58-63, column 5 lines 36-41, column 6 lines 48-50);

a filter associated with the applications programming interface and each respective network vulnerability analysis program for filtering the system object model database and exporting only the required data requirements to each network vulnerability analysis program (column 5 lines 36-60, column 7 lines 1-9); and

a processor for correlating the data results obtained from each network vulnerability analysis program after analyzing the network to determine the security posture of the network (column 5 lines 55-58, column 6 lines 44-47).

Regarding claim 2, Gleichauf discloses:

A method according to claim 1, and further comprising the step of importing the system object model database to the network vulnerability analysis programs via an integrated application programming interface (column 2 lines 58-63, column 5 lines 36-41, column 6 lines 48-50).

Regarding claim 4, Gleichauf discloses:

A method according to claim 1, and further comprising the step of establishing a class hierarchy to define components of the network vulnerability analysis programs that share common and programming traits (column 6 lines 62-65).

Regarding claim 6, Gleichauf discloses:

A method according to claim 1, and further comprising the step of running the network vulnerability assessment/risk analysis programs to obtain data results pertaining to network system details, network topologies, node level vulnerabilities and network level vulnerabilities (column 5 lines 29-31, column 5 lines 55-67, column 6 lines 5-47).

Regarding claim 8, Gleichauf discloses:

A method according to claim 7, and further comprising the step of exporting the system object model database to the network vulnerability assessment/risk analysis programs via an integrated application programming interface (column 2 lines 58-63, column 5 lines 36-41, column 6 lines 48-50).

Regarding claim 10, Gleichauf discloses:

A method according to claim 7, and further comprising the step of establishing a class hierarchy to define components of the network vulnerability analysis programs that share common data and programming traits (column 6 lines 62-65).

Regarding claim 12, Gleichauf discloses:

A method according to claim 7, and further comprising the step of running the network vulnerability analysis programs to obtain data results pertaining to network system details, network topologies, node level vulnerabilities and network level vulnerabilities (column 5 lines 29-31, column 5 lines 55-67, column 6 lines 5-47).

Regarding claim 14, Gleichauf discloses:

A computer program according to claim 13, and further comprising instructions for displaying an integrated application programming interface, and exporting the system object model database to the network vulnerability analysis programs via the integrated application programming interface (column 2 lines 58-63, column 5 lines 36-41, column 6 lines 48-50).

Regarding claim 16, Gleichauf discloses:

A computer program according to claim 13, and further comprising instructions for establishing a class hierarchy to define components of the network vulnerability analysis programs that share common data and programming traits (column 6 lines 62-65).

Regarding claim 18, Gleichauf discloses:

A computer program according to claim 13, and further comprising instructions for running the network vulnerability analysis programs to obtain data results that

pertain to network system details, network topologies, node level vulnerabilities and network level vulnerabilities (column 5 lines 29-31, column 5 lines 55-67, column 6 lines 5-47).

Regarding claim 20, Gleichauf discloses:

A computer program according to claim 19, and further comprising instructions for displaying an integrated application programming interface, and exporting the system object model database to the network vulnerability analysis programs via the integrated application programming interface (column 2 lines 58-63, column 5 lines 36-41, column 6 lines 48-50).

Regarding claim 22, Gleichauf discloses:

A computer program according to claim 19, and further comprising instructions for establishing a class hierarchy to define components of the network vulnerability analysis programs that share common data and programming traits (column 6 lines 62-65).

Regarding claim 24, Gleichauf discloses:

A computer program according to claim 19, and further comprising instructions for running the network vulnerability analysis programs to obtain data results that pertain to network system details, network topologies, node level vulnerabilities and

network level vulnerabilities (column 5 lines 29-31, column 5 lines 55-67, column 6 lines 5-47).

Regarding claim 29, Gleichauf discloses:

A data processing system according to claim 25, wherein said database further comprises an object oriented class hierarchy to define components of the network vulnerability analysis programs that share common data and programming traits (column 6 lines 62-65).

Regarding claim 35, Gleichauf discloses:

A data processing system according to claim 31, wherein said database further comprises an object oriented class hierarchy to define components of the network vulnerability analysis programs that share common data and programming traits (column 6 lines 62-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3,9,15,21,26,27,28, 32, 33, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (U.S. 6,415,321) in view of Mayo et al. (U.S. 5,751,965).

Regarding claim 3, Gleichauf discloses a method of assessing the security posture of a network comprising the steps of creating a system object model database, exporting this database to vulnerability analysis programs, and correlating the data results from these network vulnerability analysis programs to determine the security posture of a network. However, Gleichauf does not explicitly describe modeling the network as a map on a graphical user interface. Mayo teaches the method of modeling the network as a map on a graphical user interface (column 2 lines 58-63, column 5 lines 49-53, column 6 lines 4-21).

Gleichauf delineates a method of gathering, storing, and correlating network vulnerability information. However, Gleichauf does not divulge the method of displaying these results. Mayo states the importance of the presentation of network information on a graphical user interface (column 1 lines 64-67, column 2 lines 1-9), and delineates a method of constructing a network map showing displaying different network attributes. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to display the network vulnerability assessment information gathered by the system of Gleichauf using the network display method of Mayo to be able to display the network vulnerability information in a clear and organized manner so

that one could better use the network vulnerability information to safeguard the network elements.

Regarding claim 9, Gleichauf discloses a method of assessing the security posture of a network comprising the steps of creating a system object model database, exporting this database to vulnerability analysis programs, and correlating the data results from these network vulnerability analysis programs to determine the security posture of a network. However, Gleichauf does not explicitly describe modeling the network as a map on a graphical user interface. Mayo teaches the method of modeling the network as a map on a graphical user interface (column 2 lines 58-63, column 5 lines 49-53, column 6 lines 4-21).

Gleichauf delineates a method of gathering, storing, and correlating network vulnerability information. However, Gleichauf does not divulge the method of displaying these results. Mayo states the importance of the presentation of network information on a graphical user interface (column 1 lines 64-67, column 2 lines 1-9), and delineates a method of constructing a network map showing displaying different network attributes. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to display the network vulnerability assessment information gathered by the system of Gleichauf using the network display method of Mayo to be able to display the network vulnerability information in a clear and organized manner so that one could better use the network vulnerability information to safeguard the network elements.

Regarding claim 15, Gleichauf discloses a computer program capable of assessing the security posture of a network comprising the steps of creating a system object model database, exporting this database to vulnerability analysis programs, and correlating the data results from these network vulnerability analysis programs to determine the security posture of a network. However, Gleichauf does not explicitly describe modeling the network as a map on a graphical user interface. Mayo teaches the method of modeling the network as a map on a graphical user interface (column 2 lines 58-63, column 5 lines 49-53, column 6 lines 4-21).

Gleichauf delineates a method of gathering, storing, and correlating network vulnerability information. However, Gleichauf does not divulge the method of displaying these results. Mayo states the importance of the presentation of network information on a graphical user interface (column 1 lines 64-67, column 2 lines 1-9), and delineates a method of constructing a network map showing displaying different network attributes. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to display the network vulnerability assessment information gathered by the system of Gleichauf using the network display method of Mayo to be able to display the network vulnerability information in a clear and organized manner so that one could better use the network vulnerability information to safeguard the network elements.

Regarding claim 21, Gleichauf discloses a computer program capable of assessing the security posture of a network comprising the steps of creating a system object model database, exporting this database to vulnerability analysis programs, and correlating the data results from these network vulnerability analysis programs to determine the security posture of a network. However, Gleichauf does not explicitly describe modeling the network as a map on a graphical user interface. Mayo teaches the method of modeling the network as a map on a graphical user interface (column 2 lines 58-63, column 5 lines 49-53, column 6 lines 4-21).

Gleichauf delineates a method of gathering, storing, and correlating network vulnerability information. However, Gleichauf does not divulge the method of displaying these results. Mayo states the importance of the presentation of network information on a graphical user interface (column 1 lines 64-67, column 2 lines 1-9), and delineates a method of constructing a network map showing displaying different network attributes. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to display the network vulnerability assessment information gathered by the system of Gleichauf using the network display method of Mayo to be able to display the network vulnerability information in a clear and organized manner so that one could better use the network vulnerability information to safeguard the network elements.

Regarding claim 26, Gleichauf discloses a data processing system for assessing the security vulnerability of a network comprising a plurality of network vulnerability analysis

programs, an applications programming interface to export the system object model database to the network vulnerability analysis programs, and a processor for correlating the data results obtained from the network vulnerability analysis programs. However, Gleichauf does not explicitly describe the applications programming interface to be a graphical user interface. Mayo teaches a network management system that maintains a database of models relating to corresponding network elements, including a user interface (Fig. 3, column 4 lines 52-60, column 5 lines 49-53). It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to use a graphical user interface described by Mayo to import the system object model database to increase the ease of operation. Using Mayo's graphical user interface to export information to network vulnerability assessment programs would increase the efficiency and user-friendliness of the system, creating a better system for determining and resolving network vulnerabilities.

Regarding claim 27, Gleichauf discloses a data processing system capable of assessing the security posture of a network comprising the steps of creating a system object model database, exporting this database to vulnerability analysis programs, and correlating the data results from these network vulnerability analysis programs to determine the security posture of a network. However, Gleichauf does not explicitly describe modeling the network as a map on a graphical user interface. Mayo teaches the method of modeling the network as a map on a graphical user interface (column 2 lines 58-63, column 5 lines 49-53, column 6 lines 4-21).

Gleichauf delineates a method of gathering, storing, and correlating network vulnerability information. However, Gleichauf does not divulge the method of displaying these results. Mayo states the importance of the presentation of network information on a graphical user interface (column 1 lines 64-67, column 2 lines 1-9), and delineates a method of constructing a network map showing displaying different network attributes. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to display the network vulnerability assessment information gathered by the system of Gleichauf using the network display method of Mayo to be able to display the network vulnerability information in a clear and organized manner so that one could better use the network vulnerability information to safeguard the network elements.

Regarding claim 28, Gleichauf discloses a method of assessing the security posture of a network comprising the steps of creating a system object model database, exporting this database to vulnerability analysis programs, and correlating the data results from these network vulnerability analysis programs to determine the security posture of a network. However, Gleichauf does not explicitly describe displaying the security posture on a graphical user interface. Mayo teaches the method of modeling the network as a map displaying the security posture and other network information on a graphical user interface (column 2 lines 58-63, column 5 lines 49-53, column 6 lines 4-21).

Gleichauf delineates a method of gathering, storing, and correlating network vulnerability information to determine the security posture of the network. However, Gleichauf does not divulge the method of displaying the security posture of the network on a graphical user interface. Mayo states the importance of the presentation of network information on a graphical user interface (column 1 lines 64-67, column 2 lines 1-9), and delineates a method of constructing a network map showing displaying different network attributes. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to display the network vulnerability assessment information gathered by the system of Gleichauf using the network display method of Mayo to be able to display the network vulnerability information in a clear and organized manner so that one could better use the network vulnerability information to safeguard the network elements.

Regarding claim 32, Gleichauf discloses a data processing system for assessing the security vulnerability of a network comprising a plurality of network vulnerability analysis programs, an applications programming interface to export the system object model database to the network vulnerability analysis programs, and a processor for correlating the data results obtained from the network vulnerability analysis programs. However, Gleichauf does not explicitly describe the applications programming interface to be a graphical user interface. Mayo teaches a network management system that maintains a database of models relating to corresponding network elements, including a user interface (Fig. 3, column 4 lines 52-60, column 5 lines 49-53). It would have been

obvious to one of ordinary skill in the art at the time the applicant's invention was made to use a graphical user interface described by Mayo to import the system object model database to increase the ease of operation. Using Mayo's graphical user interface to export information to network vulnerability assessment programs would increase the efficiency and user-friendliness of the system, creating a better system for determining and resolving network vulnerabilities.

Regarding claim 33, Gleichauf discloses a data processing system capable of assessing the security posture of a network comprising the steps of creating a system object model database, exporting this database to vulnerability analysis programs, and correlating the data results from these network vulnerability analysis programs to determine the security posture of a network. However, Gleichauf does not explicitly describe modeling the network as a map on a graphical user interface. Mayo teaches the method of modeling the network as a map on a graphical user interface (column 2 lines 58-63, column 5 lines 49-53, column 6 lines 4-21).
Gleichauf delineates a method of gathering, storing, and correlating network vulnerability information. However, Gleichauf does not divulge the method of displaying these results. Mayo states the importance of the presentation of network information on a graphical user interface (column 1 lines 64-67, column 2 lines 1-9), and delineates a method of constructing a network map showing displaying different network attributes. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to display the network vulnerability assessment information

gathered by the system of Gleichauf using the network display method of Mayo to be able to display the network vulnerability information in a clear and organized manner so that one could better use the network vulnerability information to safeguard the network elements.

Regarding claim 34, Gleichauf discloses a method of assessing the vulnerability posture of a network comprising the steps of creating a system object model database, exporting this database to vulnerability analysis programs, and correlating the data results from these network vulnerability analysis programs to determine the security posture of a network. However, Gleichauf does not explicitly describe displaying the vulnerability posture on a graphical user interface. Mayo teaches the method of modeling the network as a map displaying the security posture and other network information on a graphical user interface (column 2 lines 58-63, column 5 lines 49-53, column 6 lines 4-21).

Gleichauf delineates a method of gathering, storing, and correlating network vulnerability information to determine the security posture of the network. However, Gleichauf does not divulge the method of displaying the security posture of the network on a graphical user interface. Mayo states the importance of the presentation of network information on a graphical user interface (column 1 lines 64-67, column 2 lines 1-9), and delineates a method of constructing a network map showing displaying different network attributes. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to display the network vulnerability

assessment information gathered by the system of Gleichauf using the network display method of Mayo to be able to display the network vulnerability information in a clear and organized manner so that one could better use the network vulnerability information to safeguard the network elements.

6. Claims 5,11,17,23,30 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (U.S. 6,415,321) in view of Smith et at. (U.S. 5,787,235).

Regarding claim 5, Gleichauf discloses a method for assessing the security posture of a network comprising the step of correlating the data results from a vulnerability assessment programs. However, Gleichauf does not explicitly describe how this data is correlated. Smith delineates a fuzzy-logic based evidence fusion tool that can be applied to network configuration analysis, modeling and assessment (column 6 lines 26-30). Smith states the tool disclosed applies fuzzy logic to telecommunication network configuration analysis, modeling and assessment. This assessment disclosed can be viewed as a network vulnerability assessment correlation. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to use Smith's method of applying fuzzy logic to network data to correlate the vulnerability assessment information provided by Gleichauf's system. The use of fuzzy logic processing allows correlation of the results from the programs into a cohesive vulnerability assessment to obtain an overall network vulnerability posture.

Regarding claim 11, Gleichauf discloses a method for assessing the security posture of a network comprising the step of correlating the data results from a vulnerability assessment programs. However, Gleichauf does not explicitly describe how this data is correlated. Smith delineates a fuzzy-logic based evidence fusion tool that can be applied to network configuration analysis, modeling and assessment (column 6 lines 26-30). Smith states the tool disclosed applies fuzzy logic to telecommunication network configuration analysis, modeling and assessment. This assessment disclosed can be viewed as a network vulnerability assessment correlation. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to use Smith's method of applying fuzzy logic to network data to correlate the vulnerability assessment information provided by Gleichauf's system. The use of fuzzy logic processing allows correlation of the results from the programs into a cohesive vulnerability assessment to obtain an overall network vulnerability posture.

Regarding claim 17, Gleichauf discloses computer program for assessing the security posture of a network comprising the step of correlating the data results from a vulnerability assessment programs. However, Gleichauf does not explicitly describe how this data is correlated. Smith delineates a fuzzy-logic based evidence fusion tool that can be applied to network configuration analysis, modeling and assessment (column 6 lines 26-30). Smith states the tool disclosed applies fuzzy logic to telecommunication network configuration analysis, modeling and assessment. This

assessment disclosed can be viewed as a network vulnerability assessment correlation. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to use Smith's method of applying fuzzy logic to network data to correlate the vulnerability assessment information provided by Gleichauf's system. The use of fuzzy logic processing allows correlation of the results from the programs into a cohesive vulnerability assessment to obtain an overall network vulnerability posture.

Regarding claim 23, Gleichauf discloses a computer program for assessing the security posture of a network comprising the step of correlating the data results from a vulnerability assessment programs. However, Gleichauf does not explicitly describe how this data is correlated. Smith delineates a fuzzy-logic based evidence fusion tool that can be applied to network configuration analysis, modeling and assessment (column 6 lines 26-30). Smith states the tool disclosed applies fuzzy logic to telecommunication network configuration analysis, modeling and assessment. This assessment disclosed can be viewed as a network vulnerability assessment correlation. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to use Smith's method of applying fuzzy logic to network data to correlate the vulnerability assessment information provided by Gleichauf's system. The use of fuzzy logic processing allows correlation of the results from the programs into a cohesive vulnerability assessment to obtain an overall network vulnerability posture.

Regarding claim 30, Gleichauf discloses a data processing system for assessing the security posture of a network comprising the step of correlating the data results from a vulnerability assessment programs. However, Gleichauf does not explicitly describe how this data is correlated. Smith delineates a fuzzy-logic based evidence fusion tool that can be applied to network configuration analysis, modeling and assessment (column 6 lines 26-30). Smith states the tool disclosed applies fuzzy logic to telecommunication network configuration analysis, modeling and assessment. This assessment disclosed can be viewed as a network vulnerability assessment correlation. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to use Smith's method of applying fuzzy logic to network data to correlate the vulnerability assessment information provided by Gleichauf's system. The use of fuzzy logic processing allows correlation of the results from the programs into a cohesive vulnerability assessment to obtain an overall network vulnerability posture.

Regarding claim 36, Gleichauf discloses a data processing system for assessing the security posture of a network comprising the step of correlating the data results from a vulnerability assessment programs. However, Gleichauf does not explicitly describe how this data is correlated. Smith delineates a fuzzy-logic based evidence fusion tool that can be applied to network configuration analysis, modeling and assessment (column 6 lines 26-30). Smith states the tool disclosed applies fuzzy logic to

telecommunication network configuration analysis, modeling and assessment. This assessment disclosed can be viewed as a network vulnerability assessment correlation. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to use Smith's method of applying fuzzy logic to network data to correlate the vulnerability assessment information provided by Gleichauf's system. The use of fuzzy logic processing allows correlation of the results from the programs into a cohesive vulnerability assessment to obtain an overall network vulnerability posture.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

KA
04/28/04

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100